AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: Brandon Hale, 1/18/2024

AMG 1/19/24

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
(Briefly describe the property to be search)
Or identify the person by name and address))
Samsung GSM SM-G965U Galaxy S9+)
IMEI 357633090381481, and extraction, and)
iPhone 11 IMEI 352907117375170, and extraction)

Case No: M-24-54-AMG

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:*(identify the person or describe property to be searched and give its location)*:

See Attachment A

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 U.S.C. § 1324(a)(1)((A)(2)	Transporting Illegal Aliens
8 U.S.C. § 1326	Reentry of Removed Aliens

The application is based on these facts:

See attached Affidavit of Special Agent Rachel L. Cathie, the Homeland Security Investigations (HSI), which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Rachel Cathie

Applicant's signature

Rachel L. Cathie
Special Agent
HSI

Sworn to before me and signed in my presence.

Date: 1/19/2024

Amanda Maxfield Green
Judge's signature

City and State: Oklahoma City, Oklahoma

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

I, Rachel L. Cathie, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing the examination of a Samsung GSM SM-G965U Galaxy S9+ IMEI 357633090381481 and an iPhone 11 IMEI 352907117375170 (hereinafter referred to as "the DEVICES") (and their associated Cellebrite extractions), as described in Attachment A, which is currently secured in the Homeland Security Investigations (HSI) Oklahoma City Office.

2. I am a Special Agent (SA) employed by the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) with Homeland Security Investigations (HSI). I have the authority to investigate violations of federal and state laws including, but not limited to, human trafficking, alien smuggling, financial crimes, narcotics smuggling, intellectual property rights violations, child pornography, weapons trafficking, and organized criminal activity. I have been employed with HSI since September 2019 and have completed the Criminal Investigative Training Program and Homeland Security Investigations Special Agent Training Program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I am currently assigned to the Oklahoma City Office in the Area of Responsibility (AOR) of the Special Agent in Charge in Dallas, Texas. I have worked with other experienced local, state, and federal law enforcement officers, as well as prosecuting attorneys, and have become familiar with

human smuggling, money laundering, criminal violations, and investigative techniques. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement personnel, interviews, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of evidence in this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the electronically stored content and information on the DEVICES (and their associated Cellebrite extractions) constitutions evidence of the commission of criminal offenses; contraband, the fruits of crime, and things otherwise criminally possessed; and property designed and intended for use, and which has been used as a means of committing criminal offenses, namely, violations of: 8 U.S.C. § 1324(a)(1)(A)(2) transporting certain aliens within the United States and 8 U.S.C. § 1326, illegal reentry (the "Subject Offenses"). Accordingly, there is probable cause to authorize the examination of the information on the DEVICES (and their associated Cellebrite extractions), as described in Attachment A for the information as described in Attachment B.

COMMON PRACTICES OF PERSONS WHO UNLAWFULLY ENGAGE IN HUMAN SMUGGLING

4. Based on my training and experience, as well as the collective training, experience, and information from other law enforcement officials, I know the following:

a. Law enforcement utilizes a wide range of investigative techniques to identify and dismantle Alien Smuggling Organizations (ASOs). These ASOs can be best

described as disciplined structured groups who have compartmentalized and insulated individual functions to maintain the integrity of their operation. ASOs can be associated with transnational criminal organizations, which have significant financial resources and counter-intelligence assets. ASOs routinely use commercial airlines, maritime vessels, railroads, commercial vehicles, hotels, couriers, and rental vehicles in furtherance of their operations. Furthermore, I know through my training and experience that timely communication is essential to facilitate alien smuggling. Such communications are commonly made using computers, electronic devices, and mobile devices such as cellular phones.

b. Alien smugglers commonly use computers, electronic devices, and cellular phones to discuss or arrange pick-up and drop-off locations in an attempt to make it difficult for law enforcement to identify or intercept their conversations. It is common for smugglers to separate their relationships from their personal or business relationships by using different phones to communicate with co-conspirators and customers. The "dirty phone" will typically be an anonymous prepaid phone or in the name of another person or business in an attempt to elude law enforcement.

c. Alien smuggling is commonly a conspiratorial crime involving the use of others to assist during the actual commission of the crime. Suspects actively need to communicate while the crime is being committed. This assistance comes in the form of other suspects, both known and unknown, who will monitor police radio traffic and alert the perpetrators of the impending arrival of law enforcement, counter surveillance or lookouts who will maintain visual surveillance on the approaches to a crime scene to alert

their associates of the presence of law enforcement, and getaway drivers who will assist perpetrators with their escape. Communications between co-conspirators is essential to successfully facilitate alien smuggling. Such communications are commonly made using computers, electronic devices, and cellular phones.

d. Alien smugglers will often attempt to conceal or destroy physical evidence, conspire with others to create alibis, boast, or brag about the commission of a crime, and/or attempt to flee the jurisdiction where the crime occurred. Communications between perpetrators and those who knowingly or unknowingly assist them is essential to the concealment of the crime. Such communications are commonly made using computers, electronic devices, and cellular phones.

BACKGROUND REGARDING COMPUTERS, CELLULAR PHONES, THE INTERNET, AND EMAIL

5. Based on information received from other law enforcement officials, I know the following:

a. Cell phone technology has revolutionized the way in which human smugglers facilitate the movement of undocumented and individuals illegally present in the United States.

b. As is the case with most digital technology, communications by way of a cell phone can be saved or stored on the cell phone used for these purposes, and even small devices can store tremendous amounts of data. Storing this information can be intentional, i.e., by saving an email as a file on the device or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be

retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a cell phone user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. I know that digital evidence, including pictures and videos, generally remains indefinitely on a digital storage device such as a cell phone until deleted or overwritten. I also know that even if a cell phone user deletes such evidence, a computer forensic expert can sometimes still recover it from the device using forensic tools months, and even years, after the fact.

6. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES as described in Attachment A and Attachment B. Such examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review any data seized pursuant to the requested warrant to locate any evidence, fruits, and instrumentalities of human smuggling.

7. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the

DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES

8. Searches and seizures of evidence from cell phones and other digital file storage devices commonly require agents to download or copy information from the

devices and their components or seize most or all devices to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Digital file storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching digital file storage devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of cell phone hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password- protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

9. In order to fully retrieve data from a cell phone, the analyst needs all digital and/or magnetic storage devices as well as the device's central processing unit. In addition,

the analyst needs all the system software, including operating systems or interfaces and hardware drivers, and application software which may have been used to create the data, whether stored on the hard drives or external media.

PROBABLE CAUSE

10. On November 21, 2023, SA I (R. Cathie) was notified by Oklahoma Highway Patrol ("OHP") that a Guatemalan Citizen, identified as Jose PAXTOR ("PAXTOR") was the driver at fault in a vehicle accident where 6 of PAXTOR's passengers died: three adults, three juveniles—and one of the passengers was a young female child left in critical condition. An OHP Trooper told SA R. Cathie that PAXTOR was taking pictures with his phone of the deceased victims at the scene while the troopers were working. An OHP Investigator, Trooper R. Hayes, told SA R. Cathie that there were two phones that belonged to PAXTOR, which were seized and later identified as the DEVICES. Trooper R. Hayes told SA R. Cathie that PAXTOR was arrested on Oklahoma State charges of manslaughter and was (and is) being held at Beckham County Jail, located at: 108 S 3rd St, Sayre, OK 73662.

11. On the same date, SAs C. Busbee and R. Cathie, with Trooper R. Hayes, interviewed PAXTOR at the Beckham County Jail. The interview was conducted in Spanish by SA C. Busbee, as PAXTOR did not speak English. Prior to the interview, PAXTOR was advised of his rights as per Miranda. PAXTOR indicated he understood his rights, waived his rights, and agreed to speak with investigators without an attorney present. PAXTOR stated he last entered the United States illegally in 2011 with the help

of a coyote[1] whom he paid $500 and lived in Los Angeles, California. PAXTOR stated that earlier in the day on November 21, 2023, he was driving from New York, NY to Los Angeles, CA. PAXTOR stated that he had left Los Angeles on Thursday, traveled through Las Vegas NV, Colorado, Missouri, and Kentucky on I-70. PAXTOR said he left New York on Sunday and the passengers in his vehicle had asked him for a ride. Initially, PAXTOR denied being paid by the passengers to transport them and stated that they only helped him with some gas money. Later, PAXTOR admitted he charged $300 per passenger to take them from New York to Los Angeles. PAXTOR stated he had not received their payments yet and would have been paid in cash upon arrival in Los Angeles. PAXTOR stated that he had made this trip (LA to NY and then back to LA) once a month for the past year and a half. PAXTOR stated that he was not being directed by anyone and organized the trips on his own. PAXTOR stated that he would ask the travelers to tell their friends to contact him if they knew of anyone who needed a ride. PAXTOR stated that the individuals in the vehicle with him on this trip were all Guatemalan except for a Mexican male he picked up in Oklahoma, and he spoke to his passengers in Spanish. PAXTOR stated he stopped at a restaurant called "El Chapin," which he believed was near a highway exit in Oklahoma, and picked up the Mexican male.[2] PAXTOR stated that the passengers couldn't find jobs in New York and wanted to go to California. PAXTOR stated that he was traveling with an iPhone that had a phone

---

[1] Based on training and experience, SA Cathie knows that "coyote" is a common slang term describing a person who illegally smuggles people across the border into the United States.

[2] The Mexican male was identified as a juvenile, illegally present in the United States.

number of (323) 672-1238 and passcode of: 7892580 and a Samsung with phone number (213) 260-5758. PAXTOR then drew the design to unlock the Samsung phone. PAXTOR gave investigators verbal consent to search both of his cellphones and his vehicle. PAXTOR could not read or write and therefore did not sign a consent form.

12. On November 30, 2023, HSI Oklahoma City and OHP Trooper R. Hayes spoke with Hugo XOL-CUC ("H. XOL-CUC") and Mauro CUC-XOL ("M. CUC-XOL") at Oklahoma Children's Hospital OU Health, with an OU Hospital employee assisting as a Spanish translator. M. CUC-XOL and H. XOL-CUC were related to the six Guatemalan passengers who were transported by PAXTOR. M. CUC-XOL told SA R. Cathie that he and his sister had arranged for their family to be transported from New York to California; M. CUC-XOL contacted the company via a WhatsApp[3] advertisement that had a picture of a white minivan and a phone number of (323) 646-3523. The white minivan used in the advertisement was almost identical to the van PAXTOR was driving when he caused the vehicle accident. SA R. Cathie asked M. CUC-XOL how he knew it was his family that was involved in the vehicle accident, and he stated he was given updates from the transport company via WhatsApp, but the updates stopped when the vehicle accident happened, and he was blocked on WhatsApp. SA R. Cathie asked how M. CUC-XOL paid for the transport, and M. CUC-XOL stated he and his sister paid $1,000 each via Zelle to a person named "Rodel Leonel Lopez" with a phone number of:

[3] WhatsApp Messenger is an internationally available freeware, cross-platform, centralized instant messaging and voice-over-IP service owned by US tech conglomerate Meta. It allows users to send text and voice messages, make voice and video calls, and share images, documents, user locations, and other content.

(540) 217-1752.[4] SA R. Cathie asked M. CUC-XOL if he knew the driver ("PAXTOR") to which M. CUC-XOL stated he did not know the driver and did not speak with him.

13. On January 3, 2024, SA R. Cathie and SA R. Belcher interviewed Sarai GONZALEZ ("GONZALEZ"), a cousin of the deceased Mexican minor male passenger (hereinafter referred to as minor victim, "MV"). GONZALEZ told the SAs that after the crash occurred, her aunt had contacted her and said that MV was missing. GONAZLEZ stated she began calling hospitals and contacted law enforcement before learning MV died in a vehicle wreck. GONZALEZ stated that MV's brother, Raul LOPEZ ("LOPEZ") had previously made arrangements with a transport company to transport MV from his home in Oklahoma City to Atlanta, GA. During the interview, GONZALEZ called LOPEZ and acted as a Spanish translator. GONZALEZ stated that LOPEZ told her that on November 21, 2023, MV was picked up at his home address in Oklahoma City and was being driven to Los Angeles, CA; MV was going to be driven to California with the other passengers first and then would be driven to Atlanta, GA and dropped off. LOPEZ stated he was going to be charged $1,100 by the transport company to pick up MV and would pay once MV was delivered to Atlanta. LOPEZ stated he found the company through a friend who had used them previously while living in Denver, Colorado. LOPEZ stated that there were several drivers working for the same company and that he was in contact with two different people from the company. LOPEZ stated he first contacted PAXTOR on November 11, 2023, and communicated by calls, messages, and audio

[4] It is common in an Alien Smuggling Operation to have several people communicating with customers and the driver may not always be the coyote or the person directly paid.

messages, mostly via WhatsApp. LOPEZ sent GONZALEZ pictures of his communications with two of the employees of the transport company, which GONZALEZ showed SA R. Cathie. One of the employees with a WhatsApp name of "Reitero" and phone number of (323) 672-1238, had been providing LOPEZ updates about the transport of MV. SA R. Cathie noticed that the WhatsApp contact photograph appeared to be PAXTOR, and the phone number was one of the numbers PAXTOR used. GONZALEZ also showed SA R. Cathie a WhatsApp conversation between LOPEZ and a WhatsApp contact named "JI" who had a phone number of (323) 320-3423. In this conversation, "JI" had sent LOPEZ photographs of PAXTOR's vehicle accident, which was the accident that killed MV. GONZALEZ told SA R. Cathie and SA R. Belcher that it was common for these transport companies to be illegitimate businesses and to take advantage of people who are illegally present in the United States. The companies tell the customers that they aren't "free" to travel and therefore, will need transportation provided.

14. PAXTOR is an alien, who had previously been removed, and is currently charged in this district with illegal reentry in a pending Criminal Complaint. All of his passengers described above are aliens. All of them entered the United States illegally. With the exception of one of them, they had been previously apprehended and released after being given instructions to appear in immigration court. Based on PAXTOR's verbal consent, soon after the seizure of the DEVICES, Cellebrite extractions (forensic copies) were made of the DEVICES. In an abundance of caution, I'm seeking this search warrant to search through those two Cellebrite extractions as well as the physical cell phones

themselves for evidence, fruits, and instrumentalities of the SUBJECT OFFENSES. Finally, SA Cathie believes evidence not only of illegally transporting aliens but also of PAXTOR's own illegal reentry offense will be on the DEVICES (and associated Cellebrite extractions). For example, map driving history from the DEVICES can shed light on where and for how long PAXTOR was illegally in the United States.

CONCLUSION

15. Based on the above information, there is probable cause to believe that violations of the SUBJECT OFFENSES were committed by PAXTOR, and that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES are located within the DEVICES (and their associated Cellebrite extractions). Therefore, I respectfully request that this Court issue a search warrant for the DEVICES (and their Cellebrite associated extractions), described in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,

Rachel L. Cathie
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on this 19th day of January, 2024

AMANDA MAXFIELD GREEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Items to Be Searched

1. A Samsung GSM SM-G965U Galaxy S9+ with IMEI 357633090381481
2. An iPhone 11 with IMEI 352907117375170
3. Cellebrite extractions of the two above phones, which have already been produced.

Such searches will be conducted by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control).

ATTACHMENT B

List of Items and Information to Be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely, violations of Title 8 United States Code Sections 1324 and 1326:

1. evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the DEVICES was accessed or used to determine the chronological context of DEVICES access, use, and events relating to crimes under investigation and to the DEVICES' user(s);
5. evidence indicating the DEVICES user's state of mind as it relates to the crimes under investigation;
6. evidence of the attachment to the DEVICES to other storage devices or similar

containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICES;
8. evidence of the times the DEVICES were used;
9. passwords, encryption keys, and other access devices that may be necessary to access the DEVICES;
10. records of or information about Internet Protocol addresses used by the DEVICES;
11. records of or information about the DEVICES' internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
12. contextual information necessary to understand the evidence described in this attachment;
13. evidence of any means of recruiting, harboring, or transporting illegal aliens
14. records, information, and items relating to any hotels, motels, truck stops, or residences that would be utilized to facilitate the transportation of unlawfully present individuals;
15. records, information, and items relating to online escort advertisements, message boards, social media platforms, or other means of advertising and promoting alien transport;
16. records, information, and items relating to the acquisition, laundering, or

possession of any proceeds related to or derived from defrauding aliens and/or transporting/harboring/facilitating the movement of illegally present or undocumented individuals in and throughout the United States.

17. records and information relating to the identity or location of the persons suspected of violating the statutes described above or victims thereof; and

18. records and information pertaining to obtaining fraudulent documents.

19. records, chats, and information discussing obtaining work illegally in the United States.

20. records, chats, and information indicating and documenting the efforts to smuggle the undocumented individuals from a foreign country into the United States;

21. records of individuals, co-conspirators, criminal associates, alien smuggling organizations, or others involved in the human smuggling event;

22. any and all phone numbers and other digital data that may contain electronic evidence of the human smuggling event;

23. any and all physical locations and location data, such as GPS, connected to the human smuggling event, such as stash houses; load houses; or pick-up, drop-off, or delivery points;

24. any and all time communications, records, or data were created and received in connection to the human smuggling event;

25. records of sources of undocumented individuals (including names, addresses, phone numbers, or any other identifying information); and

26. any and all evidence and documentation of payments, bank transactions, checks, credit card bills, account information, and other financial records connected to the human smuggling events.